A new software tool helps defend industrial control system networks against cyber attack. It makes it easier for operators to find and investigate anomalies that may threaten security.

## Helping utilities monitor for network security

By Nicole Stricker, *INL Communications & Governmental Affairs*

The name Sophia may conjure memories of the silver screen siren, but Idaho National Laboratory's Sophia tool has a different type of allure. The software sentry offers an easy, elegant way to help network operators detect intruders and other anomalies. Developers named the software using the Greek word for wisdom because that's what it provides to network administrators watching for cybersecurity threats.

Sophia passively monitors communication pathways in a static computer network. It flags new types of conversations so operators can decide if a threat is present. The tool was popular with initial users — a handful of utilities and the vendors that sell utility control systems. A second stage of testing involved dozens of companies. INL is now evaluating deployment of the technology to industry, and an August demonstration is showing how well Sophia works with several other cybersecurity tools.

**Sophia developer Gordon Rueff demonstrates the software in the Computer Assisted Virtual Environment (CAVE) at the Center for Advanced Energy Studies.**

"It really is the flagship," said David Kuipers, a program manager with the National SCADA Test Bed Program at INL, which is funded by the Department of Energy's Office of Electricity Delivery & Energy Reliability (DOE-OE) to perform research and development of cybersecurity technology for the energy industry. "It's the first technology of this group that will be transitioned to industry."

**The need for security**

Computer systems that run critical infrastructure such as power grids have been around for a long time. Historically, control systems running energy sector facilities didn't require much security because they were isolated from the outside world. But not anymore.

Such control systems are becoming more connected to the Internet via company computer networks. Administrators charged with securing these systems have a big task. They must maintain situational awareness of dozens or hundreds of computer systems that are constantly talking to each other.

The standard security software used on millions of home and office computers could help. But control system networks have unique characteristics that lend themselves to better tools, if someone would just develop them.

"That started happening seven or eight years ago," said Gordon Rueff, who led Sophia's development with INL colleagues Jared Verba, Kenneth Rohde and Corey Thuen.

"Until recently there wasn't much of a market for security tools or even situational awareness tools inside a control system because your control system was here, your Internet was over here, and they didn't talk," he said. "That's no longer the case. Now users have to think about cybersecurity."

For years, INL's critical infrastructure protection experts have been helping industry do just that. With funding support from both DOE-OE and the U.S. Department of Homeland Security, INL has built world-class cybersecurity capabilities.

INL's unique experience, infrastructure and expertise enable full-scale vulnerability assessments of industry supervisory control and data acquisition (SCADA) systems, cybersecurity evaluations of communications protocols and devices, and development of advanced training programs for industry and government.

**A constant, passive observer**

The first step of a control system vulnerability assessment often requires INL experts to map a company's entire network to locate the myriad devices and communication pathways.

The Sophia project began three years ago as a tool to automate that task for static networks — systems whose communication patterns are fairly fixed. Once the software develops a fingerprint for a given system, Sophia operates passively in the background and observes communications across the entire network. Anything out of the ordinary triggers an alert.

If your body had a sentry like Sophia, it might be able to detect the first whispers of a viral invasion before the bug could do enough damage to make you sick. It could also tell if you simply inhaled a bit of dust. Similarly, Sophia detects new network devices or communication pathways that may signal an intruder's presence early enough to thwart harm to the system.

"We'd like to know if a new host shows up or if two systems start communicating in a way they didn't before," said Rueff.

If Sophia detects something suspicious, it simply alerts the operator or network administrator, who can then investigate. The software lets the human operator evaluate new activity — it doesn't attempt to decide if the novelty is threatening.

"Sophia doesn't try to make that distinction, it just says, 'Hey, there's a new device,' or 'You've got a new communication pathway; you need to figure out what it is,'" Rueff said. "It could be something as simple as someone installed a new unit that is supposed to be there."

***DOE and industry stakeholders visited INL to see how Sophia works with other cyber security software tools developed by the lab and others.***

**Feedback from utilities**

To assess the real-world usefulness of such a tool, the INL developers talked with a few utilities and control system vendors. They liked the idea and offered to try out the software. Idaho Falls Power was one of the participating utilities.

"Idaho Falls Power … found it to be a great asset to our utility," said Mark Reed, the utility's generation superintendent at the time. "Sophia adds the characteristics of a full time employee.... We found it to be very robust, easy to install, and most importantly easy to use."

Austin Energy also participated in the proof-of-concept effort. "Austin Energy is pleased that INL has proactively begun development of its Sophia tool," said Andy Ibarra, the utility's manager of automation systems. "This functionality enhances our ability to properly secure and monitor our … systems."

With feedback from the initial testing, the developers entered development and testing about two years ago. About 30 companies are participating by downloading and using the software, and providing feedback so developers can enhance it. The testing phase is now wrapping up, and INL is evaluating avenues to make the tool available to industry.

"The whole idea is to come up with tools that can be transitioned to industry," said Kuipers.

(*Posted Aug. 30, 2012*)

Feature Archive